equal or greater protection from the prohibited practices set forth in §317.3.

§317.5 Severability.

The provisions of this Rule are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

PART 318—HEALTH BREACH NOTIFICATION RULE

Sec.

AUTHORITY: Public Law 111-5, 123 Stat. 115 (2009).

SOURCE: 74 FR 42980, Aug. 25, 2009, unless otherwise noted.

§318.1 Purpose and scope.

(a) This part, which shall be called the ''Health Breach Notification Rule,'' implements section 13407 of the American Recovery and Reinvestment Act of 2009. It applies to foreign and domestic vendors of personal health records, PHR related entities, and third party service providers, irrespective of any jurisdictional tests in the Federal Trade Commission (FTC) Act, that maintain information of U.S. citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity.

(b) This part preempts state law as set forth in section 13421 of the American Recovery and Reinvestment Act of 2009.

§318.2 Definitions.

(a) *Breach of security* means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.

(b) *Business associate* means a business associate under the Health Insurance Portability and Accountability Act, Public Law 104-191, 110 Stat. 1936, as defined in 45 CFR 160.103.

(c) *HIPAA*-covered entity means a covered entity under the Health Insurance Portability and Accountability Act, Public Law 104-191, 110 Stat. 1936, as defined in 45 CFR 160.103.

(d) *Personal health record* means an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

(e) *PHR identifiable health information* means ''individually identifiable health information,'' as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information:

(1) That is provided by or on behalf of the individual; and

(2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

(f) *PHR related entity* means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that:

(1) Offers products or services through the Web site of a vendor of personal health records;

(2) Offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records; or

(3) Accesses information in a personal health record or sends information to a personal health record.

(g) *State* means any of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa and the Northern Mariana Islands.